Abstract

WO0182549

The invention relates to a method and a device for dynamically controlling access, e.g. a session manager. In said method and device, the logon of at least one client is registered, at least one IP address is allocated to said client and access to the IP address is withdrawn from said client(s) once a predeterminable time period has elapsed and/or based on a predeterminable condition.

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
1. November 2001 (01.11.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/82549 A2

(51) Internationale Patentklassifikation[7]: H04L 29/00

(21) Internationales Aktenzeichen: PCT/EP01/04524

(22) Internationales Anmeldedatum:
20. April 2001 (20.04.2001)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
100 21 255.7 20. April 2000 (20.04.2000) DE
100 43 258.1 25. August 2000 (25.08.2000) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **IP-CONTROL GMBH I. GR.** [DE/DE]; Falkensteinstrasse 17, 10997 Berlin (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **RÜFFLER, Dieter** [DE/DE]; Falkensteinstrasse 17, 10997 Berlin (DE).

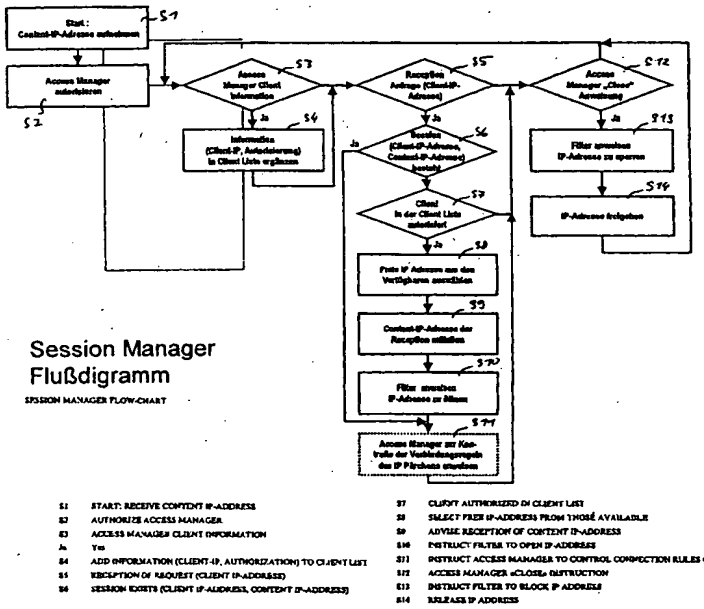
(74) Anwalt: **KÖRBER, Martin**; Mitscherlich & Partner, Postfach 33 06 09, 80066 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND DEVICE FOR DYNAMICALLY CONTROLLING ACCESS TO INTERNET SERVICES

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR DYNAMISCHEN ZUGRIFFSKONTROLLE VON INTERNET-DIENSTEN



(57) Abstract: The invention relates to a method and a device for dynamically controlling access, e.g. a session manager. In said method and device, the logon of at least one client is registered, at least one IP address is allocated to said client and access to the IP address is withdrawn from said client(s) once a predeterminable time period has elapsed and/or based on a predeterminable condition.

(57) Zusammenfassung: Die vorliegende Erfindung betrifft ein Verfahren und eine Vorrichtung zur dynamischen Zugriffskontrolle, wie z.B. einen Session Manager, bei denen die Anmeldung mindestens eines Clients registriert wird, dem Client mindestens eine IP-Adresse zugeteilt wird und nach Ablauf eines vorbestimmbaren Zeitraums und/oder in Abhängigkeit einer vorbestimmbaren Bedingung dem mindestens einem Client der Zugang zur IP-Adresse entzogen wird.

WO 01/82549 A2

LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) **Bestimmungsstaaten** *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Verfahren und Vorrichtung zur dynamischen Zugriffskontrolle von Internetdiensten

Beschreibung

Die Erfindung befasst sich mit einem Verfahren und einer Vorrichtung zur dynamischen Zugriffskontrolle von Internetdiensten.

Bisher findet die Abrechnung von Internetdienstleistungen wie in **Figur 9** schematisch dargestellt statt. Ein erster Client C1 und ein zweiter Client C2, die hinter einer gemeinsamen Firewall FW liegen, treten mit einem Content Server S in Kontakt. Es sind vier Schichten des OSI-Referenzmodells dargestellt. In der Sicherungsschicht A, die der Schicht 2 des OSI-Referenzmodells entspricht, besteht keine Verbindung zwischen den Clients C1, C2 und Content Server S. Der Schicht 3 im OSI-Referenzmodell entspricht die Netzwerkschicht B, der Schicht 4 die Transportschicht C und der Schicht 7 die Anwendungsschicht D. In der Netzwerkschicht B besteht nur eine einzige Verbindung 1 zwischen der Firewall FW und dem Content Server S. Dagegen besteht in den beiden oberen Schichten C, D jeweils eine Vebindung 2a, 2b und 3a, 3b zwischen den einzelnen Clients C1, C2 und dem Content Server S. Die Bezahlung erfolgt indirekt. Dazu wird beispielsweise beim Verbindungsaufbau zwischen dem ersten Client C1 und dem Content Server S auf Anfrage die Kreditkartennummer des ersten Client C1 mitgeteilt. Dieser weist einen ersten Payment Server PS über eine Verbindung 4 an, die Zahlung vorzunehmen. Die Abrechnung erfolgt über dan ersten Payment Server PS, hier ein Kreditkarteninstitut des ersten Clients C1. Dieses steht jedoch nicht in Verbindung mit dem Content Server S. Eine Vorabbezahlung der Dienste des Content Servers S durch den ersten Client C1 erfolgt nicht, sondern ihm wird nach Abschluss der Session sein Kreditkartenkonto belastet. Eine andere Möglichkeit ist es, die Bezahlung über die Telefonrechnung, wie bspw. für den zweiten Client C2 gezeigt, vorzunehmen. Der zweite Client C2 steht dazu mit einem zweiten Payment Server PS über eine Verbindung 5 in Kontakt. Dabei kann es jedoch Probleme für den Betreiber des Content Server S geben, wenn der zweite Client C2 die Kosten für die Session nicht bezahlen möchte.

Die Aufgabe der Erfindung ist es, ein Verfahren und eine Vorrichtung zur Verfügung zu stellen, die eine Fakturierung von Internetdiensten ermöglicht, nachdem eine Bezahlung des Client an den Betreiber eines Content Servers erfolgt ist.

Diese Aufgabe wird durch ein Verfahren zur dynamischen Zugriffskontrolle gemäß Anspruch 1 gelöst, bei dem die Anmeldung mindestens eines Clients auf einem Datenverarbeitungssystem, wie z.B. einem Content Server oder einem Session Manager registriert wird, dem Client mindestens eine IP-Adresse zugeteilt wird, und nach Ablauf eines vorbestimmbaren Zeitraums und/oder in Abhängigkeit einer vorbestimmbaren Bedingung dem mindestens einem Client der Zugang zur IP-Adresse entzogen wird.

Vorteilhafte Weiterbildungen sind Gegenstand der Unteransprüche. Vorteilhafterweise umfaßt das erfindungsgemäße Verfahren die folgenden weiteren Schritte: Absenden eines Verbindungsaufbauwunsches eines Client aus einem z.B. Internetprotokoll-basierten Kommunikationsnetz, Entgegennahme des Verbindungsaufbauwunsches durch einen Session Manager, und Anbieten eines Zahlungsmittels durch den Session Manager an den Client zur Abwicklung durch einen Payment Server. Dabei erfaßt das erfindungsgemäße Verfahren vorteilhafterweise weiterhin den Schritt der Übermittlung einer Weisung des Session Manager an einen Access Rooter Manager, eine dynamische Konfiguration eines Datenpfades oder Zugangsrechtes auf einem den Datenpfad kontrollierenden Access Rooter aufzubauen, der den Zugang des Client zu einem Content Server ermöglicht. Dabei umfaßt das erfindungsgemäße Verfahren vorteilhafterweise weiterhin den Schritt der Übertragung der öffentlichen IP-Adresse des Content Server auf IP-Adressen zur Verwaltung durch den Access Rooter. Vorteilhafterweise umfaßt das erfindungsgemäße Verfahren weiterhin den Schritt der automatischen Aktivierung einer Umleitung und des damit verbundenen Datenpfades am Anfang einer Session, so daß der Client durch den Access Rooter auf den Content Server zugreifen kann. Vorteilhafterweise umfaßt das erfindungsgemäße Verfahren weiterhin den Schritt der Abbildung der Domain-Komponente eines Content Server URLs durch den Session Manager auf die für die Umleitung reservierte IP-Adresse des stellvertretenden Access Rooter. Vorteilhafterweise umfaßt das erfindungsgemäße Verfahren weiterhin den Schritt der Aufrechterhaltung der Umleitung und des damit verbundenen Datenpfades während der Laufzeit einer Session, so daß der Client durch den Access Rooter auf den Content Server zugreifen kann, solange ein autorisiertes und gedecktes Budget für ein Ereignis, eine Zeit- und/oder eine Volumeneinheit existiert. Vorteilhafterweise umfaßt das erfindungsgemäße Verfahren weiterhin den Schritt der automatischen Deaktivierung der Umleitung und des damit verbundenen Datenpfades am Ende der Session, so daß der Client nicht weiter durch den Access Rooter auf den Content Server zugreifen kann. Vorteilhafterweise fragt der Session Manager vor Beendigung der Verbindung den Client, ob er die Session verlängern möchte, und fordert ihn auf, dafür zu bezahlen. Vorteilhafterweise verlängert dabei der Session Manager die Session, ohne die Umleitung zum Content Server zu

ändern und hält damit den Datenpfad durch den Access Rooter offen, falls der Client die Verlängerung bezahlt hat. Vorteilhafterweise werden zur Bezahlung vorausbezahlte Geldinstrumente wie Geldkarte oder Calling Card verwendet. Vorteilhafterweise ist zwischen dem Access Rooter und dem Content Server ein Server Proxy angeordnet, der mehrere Ethernet-Karten aufweist.

Die vorliegende Erfindung betrifft weiterhin eine Computersoftware zur dynamischen Zugriffskontrolle, die wenn sie in einem oder mehreren Speichern von Datenverarbeitungseinrichtungen eines Kommunikationsnetzes gespeichert ist, dazu ausgelegt ist, die oben erwähnten Schritte des erfindungsgemäßen Verfahrens durchzuführen.

Die obige Aufgabe wird weiterhin durch eine Vorrichtung zur dynamischen Zugriffskontrolle, insbesondere einen Session Manager, gemäß Anspruch 14, für mindestens einen Client eines Datenverarbeitungssystems gelöst, mit einer Einrichtung zur Vergabe mindestens einer IP-Adresse für den mindestens einen Client in Abhängigkeit eines vorbestimmbaren Zeitraums und/oder in Abhängigkeit einer vorbestimmbaren Bedingung, insbesondere eines Befehls oder eines e-mails. Vorteilhafterweise umfaßt die erfindungsgemäße Vorrichtung eine Einrichtung zur Entgegennahme eines durch einen Client aus einem z.B. Internetprotokoll basierten Kommunikationsnetz abgesendeten Verbindungsaufbauwunsches, und eine Einrichtung zum Anbieten eines Zahlungsmittels an den Client zur Abwicklung durch einen Payment Server. Vorteilhafterweise umfaßt die erfindungsgemäße Vorrichtung weiterhin eine Einrichtung zur Bereitstellung und Übermittlung einer Weisung an einen Access Rooter Manager, eine dynamische Konfiguration eines Datenpfades oder Zugangsrechts auf einem den Datenpfad kontrollierenden Access Rooter aufzubauen, der den Zugang des Client zu einem Content Server ermöglicht. Vorteilhafterweise umfaßt die erfindungsgemäße Vorrichtung eine Einrichtung zur Übertragung der öffentlichen IP-Adresse des Content Server auf IP-Adressen zur Verwaltung durch den Access Rooter. Die erfindungsgemäße Vorrichtung umfaßt weiterhin vorteilhafterweise eine Einrichtung zur automatischen Aktivierung einer Umleitung und des damit verbundenen Datenpfades am Anfang einer Session, so daß der Client durch den Access Rooter auf den Content Server zugreifen kann. Vorteilhafterweise umfaßt die erfindungsgemäße Vorrichtung weiterhin eine Einrichtung zur Abbildung der Domain-Komponente eines Content Server URLs auf die für die Umleitung reservierte IP-Adresse des stellvertretenden Access Rooter.

Vorteilhafterweise umfaßt die erfindungsgemäße Vorrichtung weiterhin eine Einrichtung zur Aufrechterhaltung der Umleitung und des damit verbundenen Datenpfades während der Laufzeit einer Session, so daß der Client durch den Access Rooter auf den Content Server zugreifen kann, solange ein autorisiertes und gedecktes Budget für ein Ereignis, eine Zeit- und/oder eine Volumeneinheit existiert.

Vorteilhafterweise umfaßt die erfindungsgemäße Vorrichtung weiterhin eine Einrichtung zur automatischen Deaktivierung der Umleitung und des damit verbundenen Datenpfades am Ende der Session, so daß der Client nicht weiter durch den Access Rooter auf den Content Server zugreifen kann. Weiterhin vorteilhafterweise umfaßt die erfindungsgemäße Vorrichtung eine Einrichtung zum Anfragen beim Client vor Beendigung der Verbindung, ob er die Session verlängern möchte und zum Auffordern, dafür zu bezahlen. Vorteilhafterweise umfaßt die erfindungsgemäße Vorrichtung weiterhin eine Einrichtung zur Verlängerung der Session, ohne die Umleitung zum Content Server zu ändern und damit zum Offenhalten des Datenpfades durch den Access Rooter, falls der Client die Verlängerung bezahlt hat.

Gemäß der vorliegenden Erfindung werden aus einem Pool jeweils andere IP-Adressen jedem erkannten individuellen Zugriff zugeteilt, der Zugriff auf jeweils dieselben geschützten Inhalte geschieht über per Session selektiv freigeschaltete IP-Adressen. Der Verkehr über die individuell vergebenen Adressen kann nach beliebigen Kriterien überwacht werden, unter anderem nach bezahlten Datenmengen, Zeitscheiben und sonstigen Ereignissen. Die An- und Abschaltung der Adressen geschieht über eine Firewall, deren Regelwerk nach Bedarf dynamisch verändert wird.

Einsatzgebiete:

Faktura kostenpflichtiger Produkte und Dienste im Internet

Vorausbezahlte oder noch zu zahlende Nutzung von Produkten und Diensten

Nutzungsverwaltung (=Sessionmanager) von Produkten und Diensten

Zeit-, volumen- und ereignisorientierte Faktura von Produkten und Diensten

Aggregierung von IP basierten Verbindungen zu Sichten auf Produkte und Dienste

Micropaymentsystem

Vorteile der Erfindung:

Unabhängigkeit von Leitungsanbietern,

beliebige Kontrollkriterien

Unabhängigkeit von den technischen Fähigkeiten der Konsumenten(rechner)

Lösung rein auf Anbieterseite hinter der schützenden Firewall

Benutzung erprobter und verbreiteter Protokolle und Komponenten: TCP-IP

Firewall, Linux

Individuelle Nutzer hinter Proxy-Servern werden erkannt

Unabhängigkeit von den angebotenen Diensttypen (Bilder, Audiodaten, etc.),

kein Eingriff in Applikationsprotokolle

Weitere Vorteile und Einzelheiten der Erfindung werden anhand der Beschreibung eines Ausführungsbeispiels zu folgenden Zeichnungen ausgeführt. Es zeigen:

Figur 1 Ein Flußdiagramm betreffend die Funktion des Session Managers der erfindungsgemäßen Zugriffskontrolle,

Figur 2 ein Diagramm, das die einzelnen Zustände einer Session, die durch einen Session Manager gesteuert wird, zeigt,

Figur 3 eine schematische Darstellung eines Systems in einem Zustand, in dem zwischen Client und Content Server keine Verbindung besteht,

Figur 4 einen Zustand des Systems aus Figur 2, in dem eine Authorisierung des Client von einem Session Manager überprüft wird,

Figur 5 einen Zustand des Systems der Figuren 2 und 3, in dem zwischen dem Client und Content Server eine Verbindung besteht,

Figur 6 einen Zustand des Systems der Figuren 2 bis 4, in dem zusätzlich eine Verbindung zwischen dem Content Server und einem weiteren Client aufgebaut wird,

Figur 7 einen Zustand des Systems der Figuren 2 bis 5, in dem der Content Server in einem Wait-Status ist, wobei kein Datentransfer vom Content Server zu einem der Clients möglich ist,

Figur 8 einen Zustand des Systems der Figuren 2 bis 6, in dem eine Authorisierung eines der Clients erfolgt, nachdem dieser einen ersten Expire erhalten hat, und

Figur 9 eine schematische Darstellung eines bisher verwendeten Bezahlungsverfahrens.

Der Ablauf des erfindungsgemäßen Verfahrens zur zeit-, volumen- und/oder ereignisorientierten Fakturierung von Internetdiensten wird schrittweise anhand der Zustände der Session in den Figuren 3 bis 8 in Verbindung mit den Diagrammen der **Figuren 1 und 2** beschrieben.

Figur 1 zeigt ein Flußdiagramm der im Session Manager ablaufenden erfindungsgemäßen Verfahrensschritte, die beispielsweise durch ein entsprechendes Computerprogramm abgearbeitet werden. Das Session Manager Programm befindet sich nach zwei Initialisierungsschritten, S1 und S2 in einer Endlosschleife und ist immer bereit, zufällig auftretende Anfragen von außen, d.h. von Clients, zu bedienen. Eine Anfrage von außen tritt entweder erstmalig auf oder wird verlängert. Eine Verlängerung wird in Schritt S4 abgearbeitet. Ansonsten muß in Schritt S5, an der Rezeption, die vollständige Information beschafft werden. Wird die Session nur verlängert, so wird direkt zu Schritt S11 übergegangen. Ansonsten müssen über mehrere Schritte die Ressourcen für die Session bereitgestellt werden. Ab Schritt S12 wird die Session abgebaut.

Der vollständige Programm- bzw. Verfahrensablauf ist wie folgt. Im Schritt S1 erfolgt der Start, d.h. eine Content-IP-Adresse wird aufgenommen. Danach wird zu Schritt S2

übergegangen, in dem der Access Manager autorisiert wird. Danach wird zu Schritt S3 übergegangen, in dem entschieden wird, ob eine Access Manager Client Information vorliegt. Wenn ja, wird zu Schritt S4 übergegangen, in dem die Information, d.h. Client-IP-Autorisierung, in der Clientliste ergänzt wird. Danach wird zu Schritt S5 übergegangen. Ist die Entscheidung im Schritt S3 negativ, wird ebenfalls zu Schritt S5 übergegangen. Im Schritt S5 wird entschieden, ob eine Anfrage mit einer Client-IP-Adresse empfangen (Rezeptionanfrage) wurde. Wenn ja, wird zu Schritt S6 übergegangen, wenn nein, wird zu Schritt S12 übergegangen. Im Schritt S6 wird beurteilt, ob eine Session (Client-IP-Adresse, Content-IP-Adresse) besteht. Wenn ja, wird zu Schritt S11 übergegangen, wenn nein wird zu Schritt S7 übergegangen. Im Schritt S7 wird überprüft, ob der Client in der Clientliste autorisiert ist. Wenn ja, wird zu Schritt S8 übergegangen, wenn nein, wird zu Schritt S12 übergegangen. Im Schritt S8 wird eine freie IP-Adresse aus den verfügbaren IP-Adressen ausgewählt. Danach wird zu Schritt S9 übergegangen, in dem eine Content-IP-Adresse dem Empfang mitgeteilt wird. Danach wird zu Schritt S10 übergegangen, in dem ein Filter angewiesen wird, die IP-Adresse zu öffnen. Danach wird zu Schritt S11 übergegangen, in dem der Access Manager zur Kontrolle der Verbindungsregeln des IP-Pärchens angewiesen wird. Danach wird zu Schritt S12 übergegangen. Im Schritt S12 wird überprüft, ob dem Access Manager eine "close"-Anweisung vorliegt, wenn ja, wird zu Schritt S13 übergegangen, wenn nein, wird zu Schritt S3 zurückgegangen. Im Schritt S13 wird der Filter angewiesen, die IP-Adresse zu sperren. Danach wird zu Schritt S14 übergegangen. In Schritt S14 wird die IP-Adresse wieder freigegeben und das Verfahren geht zurück zu Schritt S3.

In Figur 3 ist der Free-Zustand I (Figur 2) des Content Servers S gezeigt. Es sind dabei die vier Schichten A-D des OSI-Referenzmodells gezeigt, die bei der Diskussion des Standes der Technik (Figur 9) schon beschrieben wurden. In der Netzwerkschicht B sind die IP-Adressen angelegt. In der darüber dargestellten Transportschicht C werden zwei verschiedene Übertragungsprotokolle verwendet. Zum einen das Transmission Control Protocol (TCP) und das User Datagram Protocol (UDP). In der Anwendungsschicht D wird eine Vielzahl von Protokollen verwendet, wobei die häufigsten das Hypertext Transport Protocol (HTTP) und das File Transfer Protocol (FTP) verwenden. Ein erster und ein zweiter Client C1, C2, mehrere Konsumenten aus einem einzigen Intranet, sind hinter einer Firewall FW verborgen und haben jeweils eine Verbindung 6a, 6b zu ihr. Der zweite Client C2 versucht über einen ersten Link 7a durch die Firewall FW einen Content Server S zu erreichen. Er gelangt jedoch nur zu einem Access Router AR, hinter dem der Content Server S verborgen ist. Zwischen dem Access Router AR und dem

Content Server S ist ein Server Proxy SP angeordnet, in dem mehrere Ethernet-Karten enthalten sind. Diese nehmen stellvertretend für den Content Server S Verbindungsaufbauwünsche entgegen. Der Content Server S ist nicht direkt erreichbar. Diese Maßnahme schützt den Inhalt vor unauthorisierten Zugriffen sowie den Content Server S vor unerfahrenem Personal. Der Access Router AR wird von einem Access Router Manager ARM gesteuert. Dieser erhält seine Weisungen von einem mit ihm verbundenen Session Manager SM. Der Session Manager SM ist mit einem Payment Server PS verbunden. Der erste Link 7a ist ein Verbindungsaufbauwunsch (vgl. Figur 1), der vom Session Manager SM entgegengenommen wird. Dies entspricht einer Get-Anfrage II in Figur 2. In der Netzwerkschicht B besteht zwischen der Firewall FW und dem Session Manager SM genau eine Verbindung 8.

Der Content Server S geht dann von seinem Free-Zustand I (Figur 2) in seinen Wait-Zustand III (Figur 2) über, während zwischen dem Session Manager SM und dem zweiten Client C2 eine Authorisierungsverbindung 9a in der Transportschicht C und der Anwendungsschicht D aufgebaut wird (vgl. Figur 1). Dies ist in **Figur 4** dargestellt, wobei der Session Manager SM eine Überprüfung der Authorisierung der Bezahlung über den Payment Server PS vornimmt. Dazu baut er eine Verbindung 10 in den Schichten B, C, D mit dem Payment Server PS auf. Beispielsweise kann es sich bei der Bezahlung um eine GeldKarte, eine Calling Card, eine Kreditkarte oder Rechnungsstellung über die Telefon- oder Energierechnung sowie ein Bankkonto handeln. Zwischen Session Manager SM und Access Router Manager ARM wird eine Verbindung 12 aufgebaut, über die der Session Manager SM dem Access Router Manager ARM Weisungen hinsichtlich der Steuerung des Access Router AR geben kann.

Sobald der Pay-Vorgang IV (Figur 2) durch den Session Manager SM festgestellt wurde, geht der Content Server S in einen Busy-Zustand V (Figur 2) über. Dies ist in **Figur 5** dargestellt. Die Authorisierungsverbindung 9a, 10 (Figur 4) besteht zu diesem Zeitpunkt schon nicht mehr, da diese nur zur Überprüfung benötigt wird, ob der zweite Client C2 für den Zugriff auf den Content Server S bezahlt hat. Der Session Manager SM hat den Access Router Manager ARM über die Verbindung 12 angewiesen, eine dynamische Konfiguration eines Datenpfades 13 auf dem Access Router AR aufzubauen. Somit wird dem zweiten Client C2 der Zugang zum Content Server S ermöglicht. Dies geschieht durch eine Übertragung der öffentlichen IP-Adresse des Content Server S auf IP-Adressen zur Verwaltung durch den Access Router AR sowie eine automtische Aktivierung einer Umleitung 14 und des damit verbundenen Datenpfades 13 am Anfang der Session. Dabei führt der Datenpfad 13 in der Netzwerkschicht B über eine Umleitung 14, wobei ein zweiter Link 7b zwischen der IP-Adresse zur Verwaltung der Session

durch den Access Router AR und dem Server Proxy SP, sowie ein dritter Link 7c zwischen dem Server Proxy SP und der nicht-öffentlichen IP-Adresse des Content Server S aufgebaut wird. Außerdem ist eine Verbindung 15 zwischen zweitem Client C2 und Content Server S über den Server Proxy SP in der Transportschicht C und in der Anwendungsschicht D erfolgt. Über die Verbindungen 13, 15 läuft der Datentransfer während der Session ab.

In einer vorab bestimmbaren Zeit vor Ablauf der Session, beispielsweise 60 Sekunden, erfolgt vom Session Manager SM eine Pay-Nachfrage VI (Figur 2) an den zweiten Client C2. Der zweite Client C2 hat dann die Möglichkeit, die Session zu verlängern. Erteilt er einen Auftrag zur Verlängerung, so überprüft der Session Manager SM über die Verbindung 10 mit dem Payment Server PS, ob eine Authorisierung vorliegt. Dabei muss jedoch nicht zwingend das gleiche Zahlungsinstrument wie beim ersten Bezahlen der Session verwendet werden. Es ist jedes andere, vom Payment Server PS angebotene Paymentsystem verwendbar. Nach einer Verlängerung der Session bleibt der Content Server S so lange im Busy-Zustand V (Figur 2), bis diese Session ausläuft, ohne durch ein weiteres Nachzahlen des zweiten Clients C2 verlängert zu werden.

In **Figur 6** wird gezeigt, wie ein zusätzliche Verbindung zwischen dem ersten Client C1 und dem Content Server S abläuft, wobei gleichzeitig noch die Verbindung des zweiten Client C2 aktiv ist. Prinzipiell erfolgt der Verbindungsaufbau wie derjenige des zweiten Client C2 mit dem Content Server S (siehe Figuren 3 und 4). Der Verbindungsaufbauwunsch wurde über die Verbindung 8 dem Session Manager SM bekannt gemacht. Danach wurde eine Authorisierungsverbindung 9b aufgebaut. Die Authorisierung erfolgt hier ebenfalls über die Verbindung 10 mit dem Payment Server PS, der ein zweites Paymentsystem zur Verfügung stellt. Ist die Authorisierung erfolgreich abgeschlossen, so wird ein zweiter Datenpfad 17 in der Transportschicht B über den Access Router AR und den Server Proxy SP zum Content Server S aufgebaut. Der Aufbau der Verbindung 18 in den beiden Schichten C, D erfolgt wie oben beschrieben beim zweiten Client C2. Das Ergebnis ist in Figur 7 dargestellt. Die zur Überprüfung der Authorisierung benötigten Verbindungen 9b, 10 werden sofort wieder abgebaut.

Verlängert der zweite Client C2 die Session nicht, so kommt es zu einem ersten Expire VII (Figur 2) und der Content Server S geht in seinen in **Figur 7** dargestellten Wait-Zustand III (Figur 2) über. Dabei bleibt der erste Link 7a, der jedoch jetzt nur noch Teil des zweiten Datenpfades 17 ist, von der Firewall FW zum Access Router AR aktiv. Jedoch wird der zweite und dritte Link 7b, 7c zwischen Access Router AR und Server

Proxy SP bzw. zwischen Server Proxy SP und Content Server S fallengelassen, was durch die Gitterstruktur der fallengelassenen Links 7b, 7c zum Ausdruck gebracht werden soll. Außerdem findet ein Timeout der Verbindungen 15 in der Transportschicht C und in der Anwendungsschicht D statt, was durch die Gitterstruktur dargestellt ist. Die Verbindung 8 zwischen Firewall FW und Session Manager SM bleibt weiterhin bestehen. Die Daten der fallengelassenen Links 7b, 7c werden während dieser Zeit vom Session Manager SM gespeichert.

Falls der zweite Client C2 einen Pay-Vorgang IV (Figur 2) während dieses Zustandes vornimmt, nimmt der Session Manager SM wieder die oben beschriebene Zahlungsauthorisierung vor. Dies ist in **Figur 8** dargestellt. Wenn die Zahlung authorisiert ist, gibt er dem Access Router Manager ARM die Weisung, den ursprünglichen Pfad 13 über die Umleitung 14 im Access Router AR wieder zu installieren. Dadurch wird die Verbindung zwischen zweitem Client C2 und Content Server S wieder in den Busy-Zustand V (Figur 2), wie während der vorangehenden Session (Figur 5), zurückversetzt. Der Datenaustausch kann dann weitergehen.

Falls nach einer gewissen, vorab bestimmbaren Zeit kein Pay-Vorgang IV (Figur 2) erfolgt, löscht der Session Manager SM die Daten für die fallengelassenen Links 7b, 7c zwischen Content Server S und Access Router AR für die vorangehende Session zwischen zweiten Client C2 und Content Server S. Dies entspricht dem zweiten Expire VIII in Figur 2. Liegt dieser Fall für beide Sessions vor, sowohl des ersten Client C1 als auch des zeiten Client C2, ist der Free-Zustand I (Figur 2) des Content Server S wieder erreicht. Somit ergibt sich die Ausgangssituation der Figur 2.

Prinzipiell ist es auch möglich, dass noch mehr Sessions gleichzeitig ablaufen. Hierbei ist es unerheblich, ob die Clients aus einem einzigen Intranet stammen, wie oben beschrieben, oder aus verschiedenen Intranets bzw. einzelnen User sind. Der Session Manager weist den Access Router Manager für jeden einzelnen Client an, einen eigenen Datenpfad durch den Access Router zu installieren. Außerdem ist es auch möglich, dass für einen Client gleichzeitig mehrere Sessions laufen. Dabei wird prinzipiell so verfahren, wie beim Aufbau von Sessions durch verschiedene Clients. Zwischen dem Client und dem Session Manager werden dann kurzfristig so viele Verbindungen aufgebaut, wie Authorisierungen für Sessions vorzunehmen sind.

Bezugszeichenliste

AR	Access Router
ARM	Access Router Manager
C1	erster Client
C2	zweiter Client
FW	Firewall
PS	Payment Server
S	Content Server
SM	Session Manager
SP	Server Proxi
1	Verbindung
2a	Verbindung
2b	Verbindung
3a	Verbindung
3b	Verbindung
4	Verbindung
5	Verbindung
6a	Verbindung
6b	Verbindung
7a	erster Link
7b	zweiter Link
7c	dritter Link
8	Verbindung
9a	Authorisierungsverbindung
9b	Authorisierungsverbindung
10	Verbindung

2. Verbindung
3. Datenpfad
4. Umleitunng
5. Verbindung

17	zweiter Datenpfad
I	Free-Zustand
II	Get-Anfrage
III	Wait-Zustand
IV	Pay-Vorgang
V	Busy-Zustand
VI	Pay-Nachfrage
VII	erster Expire
VIII	zweiter Expire
A	Sicherungsschicht
B	Netzwerkschicht
C	Transportschicht
D	Anwendungsschicht

Patentansprüche

1. Verfahren zur dynamischen Zugriffskontrolle, bei dem die Anmeldung mindestens eines Clients auf einem Datenverarbeitungssystem, wie z.B. einem Content Server oder einem Session Manager, registriert wird, dem Client mindestens eine IP-Adresse zugeteilt wird, und nach Ablauf eines vorbestimmbaren Zeitraums und/oder in Abhängigkeit einer vorbestimmbaren Bedingung dem mindestens einen Client der Zugang zur IP-Adresse entzogen wird.

2. Verfahren gemäß Anspruch 1,
gekennzeichnet durch die Schritte
Absenden eines Verbindungsaufbauwunsches eines Client (C1, C2) aus einem z.B. Internet Protocol basierten Kommunikationsnetz;
Entgegennahme des Verbindungsaufbauwunsches durch einen Session Manager (SM);
Anbieten eines Zahlungsmittels durch den Session Manager (SM) an den Client (C1, C2), zur Abwicklung durch einen Payment Server (PS).

3. Verfahren gemäß Anspruch 2,
gekennzeichnet durch den Schritt
Weisung des Session Manager (SM) an einen Access Router Manager (ARM) eine dynamische Konfiguration eines Datenpfades (13) oder Zugangsrechts auf einem den Datenpfad (13) kontrollierenden Access Router (AR) aufzubauen, der den Zugang des Client (C1, C2) zu einem Content Server (S) ermöglicht.

4. Verfahren gemäß Anspruch 3,
gekennzeichnet durch den Schritt
Übertragung der öffentlichen IP-Addresse des Content Server (S) auf IP-Adressen zur Verwaltung durch den Access Router (AR).

5. Verfahren gemäß Anspruch 4,
gekennzeichnet durch den Schritt

Automatische Aktivierung einer Umleitung (11) und des damit verbundenen Datenpfades (13) am Anfang einer Session, so dass der Client (C1, C2) durch den Access Router (AR) auf den Content Server (S) zugreifen kann.

6. Verfahren gemäß Anspruch 5,
gekennzeichnet durch den Schritt
Abbildung der Domain-Komponente eines Content Server URLs durch den Session Manager (SM) auf die für die Umleitung reservierte IP-Adresse des stellvertretenden Access Router (AR).

7. Verfahren gemäß Anspruch 6,
gekennzeichnet durch den Schritt
Aufrechterhaltung der Umleitung (14) und des damit verbundenen Datenpfades (13) während der Laufzeit einer Session, so dass der Client (C1, C2) durch den Access Router (AR) auf den Content Server (S) zugreifen kann solange ein authorisiertes und gedecktes Budget für ein Ereignis, eine Zeit- und/oder Volumeneinheit existiert.

8. Verfahren gemäß Anspruch 7,
gekennzeichnet durch den Schritt
Automatische Deaktivierung der Umleitung (14) und des damit verbundenen Datenpfades (13) am Ende der Session, so dass der Client (C1, C2) nicht weiter durch den Access Router (AR) auf den Content Server (S) zugreifen kann.

9. Verfahren nach Anspruch 8,
dadurch gekennzeichnet, dass
der Session Manager (SM) vor Beendigung der Verbindung den Client (C1, C2) fragt, ob er die Session verlängern möchte und ihn auffordert, dafür zu bezahlen.

10. Verfahren nach Anspruch 9,
dadurch gekennzeichnet, dass

der Session Manager (SM) die Session verlängert ohne die Umleitung zum Content Server (S) zu ändern und damit den Datenpfad (13) durch den Access Router (AR) offen hält, falls der Client (C1, C2) die Verlängerung bezahlt hat.

11. Verfahren nach einem der Ansprüche 2 bis 10,
dadurch gekennzeichnet, dass
zur Bezahlung vorausbezahlte Geldinstrumente wie GeldKarte oder Calling Card verwendet werden.

12. Verfahren nach einem der Ansprüche 2 bis 11,
dadurch gekennzeichnet, dass
zwischen dem Access Router (AR) und dem Content Server (S) ein Server Proxy (SP) angeordnet ist, der mehrere Ethernet-Karten aufweist.

13. Computersoftware zur dynamischen Zugriffskontrolle, die wenn sie in einem oder mehreren Speichern von Datenverarbeitungseinrichtungen eines Kommunikationsnetzes gespeichert ist, dazu ausgelegt ist, die Schritte gemäß einem der Ansprüche 1 bis 12 durchzuführen.

14. Vorrichtung zur dynamische Zugriffskontrolle, insbesondere ein Session Manager, für mindestens einen Client eines Datenverarbeitungssystems, mit einer Einrichtung zur Vergabe mindestens einer IP-Adresse für den mindestens einen Client in Abhängigkeit eines vorbestimmbaren Zeitraums und/oder in Abhängigkeit einer vorbestimmbaren Bedingung, insbesondere eines Befehls oder eines e-mails.

15. Vorrichtung gemäß Anspruch 14,
gekennzeichnet durch
eine Einrichtung zur Entgegennahme eines durch einen Client (C1, C2) aus einem z.B. Internet Protocol basierten Kommunikationsnetz abgesendeten Verbindungsaufbauwunsches (SM); und

einer Einrichtung zum Anbieten eines Zahlungsmittels an den Client (C1, C2), zur Abwicklung durch einen Payment Server (PS).

16. Vorrichtung gemäß Anspruch 15,
gekennzeichnet durch
eine Einrichtung zur Bereitstellung und Übermittlung einer Weisung an einen Access Router Manager (ARM) eine dynamische Konfiguration eines Datenpfades (13) oder Zugangsrechts auf einem den Datenpfad (13) kontrollierenden Access Router (AR) aufzubauen, der den Zugang des Client (C1, C2) zu einem Content Server (S) ermöglicht.

17. Vorrichtung gemäß Anspruch 16,
gekennzeichnet durch
eine Einrichtung zur Übertragung der öffentlichen IP-Addresse des Content Server (S) auf IP-Adressen zur Verwaltung durch den Access Router (AR).

18. Vorrichtung gemäß Anspruch 17
gekennzeichnet durch
eine Einrichtung zur automatischen Aktivierung einer Umleitung (11) und des damit verbundenen Datenpfades (13) am Anfang einer Session, so dass der Client (C1, C2) durch den Access Router (AR) auf den Content Server (S) zugreifen kann.

19. Vorrichtung gemäß Anspruch 18,
gekennzeichnet durch
eine Einrichtung zur Abbildung der Domain-Komponente eines Content Server URLs auf die für die Umleitung reservierte IP-Adresse des stellvertretenden Access Router (AR).

20. Vorrichtung gemäß Anspruch 19,
gekennzeichnet durch
eine Einrichtung zur Aufrechterhaltung der Umleitung (14) und des damit verbundenen Datenpfades (13) während der Laufzeit einer Session, so dass der Client (C1, C2) durch

den Access Router (AR) auf den Content Server (S) zugreifen kann solange ein authorisiertes und gedecktes Budget für ein Ereignis, eine Zeit- und/oder Volumeneinheit existiert.

21. Vorrichtung gemäß Anspruch 20,
gekennzeichnet durch
eine Einrichtung zur automatische Deaktivierung der Umleitung (14) und des damit verbundenen Datenpfades (13) am Ende der Session, so dass der Client (C1, C2) nicht weiter durch den Access Router (AR) auf den Content Server (S) zugreifen kann.

22. Vorrichtung nach Anspruch 21,
gekennzeichnet durch
eine Einrichtung zum Anfragen beim Client (C1, C2) vor Beendigung der Verbindung, ob er die Session verlängern möchte und zum Auffordern, dafür zu bezahlen.

23. Vorrichtung nach Anspruch 22,
gekennzeichnet durch
eine Einrichtung zur Verlängerung der Session ohne die Umleitung zum Content Server (S) zu ändern und damit zum Offenhalten des Datenpfades (13) durch den Access Router (AR), falls der Client (C1, C2) die Verlängerung bezahlt hat.

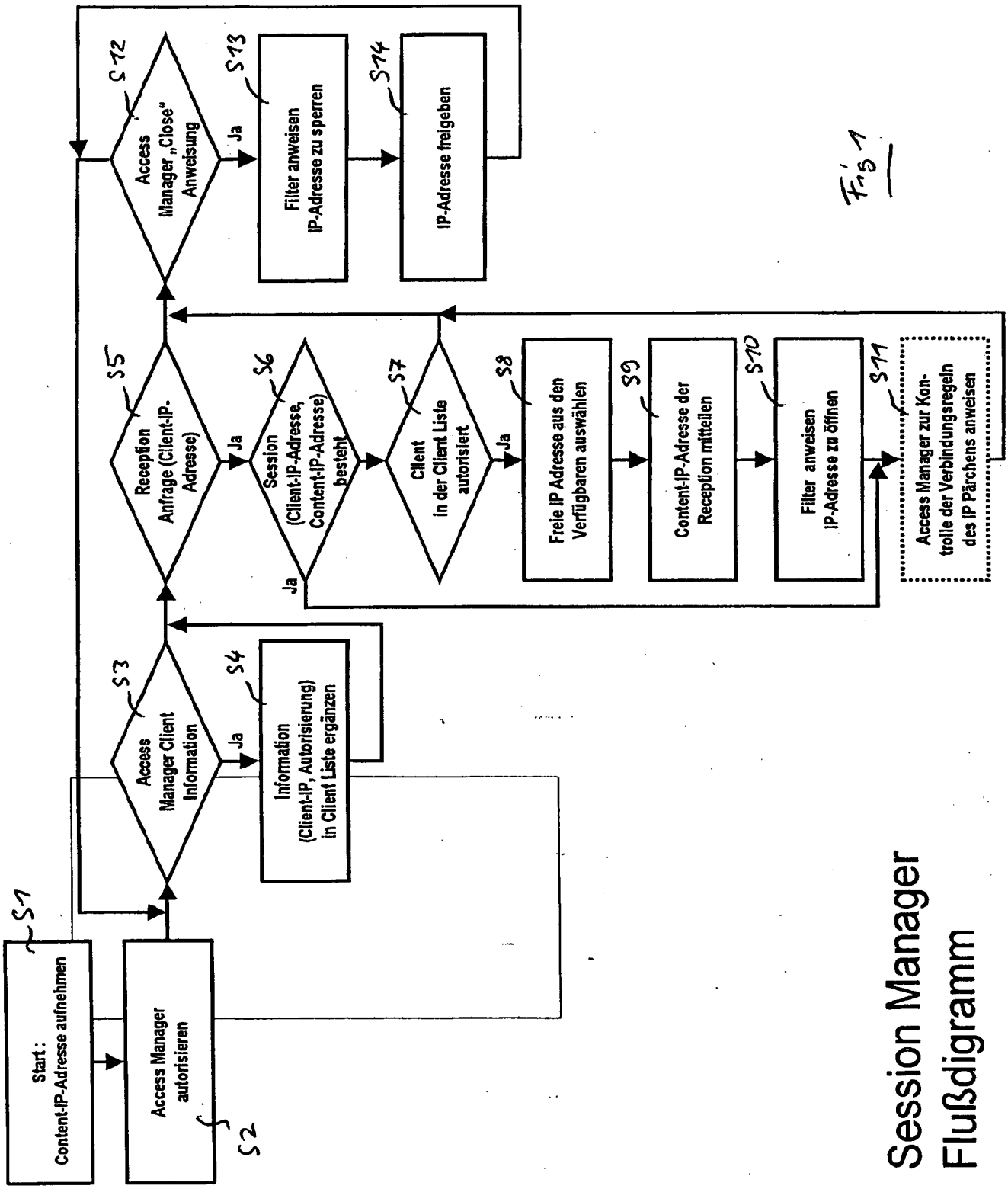


Fig 1

Session Manager
Flußdigramm

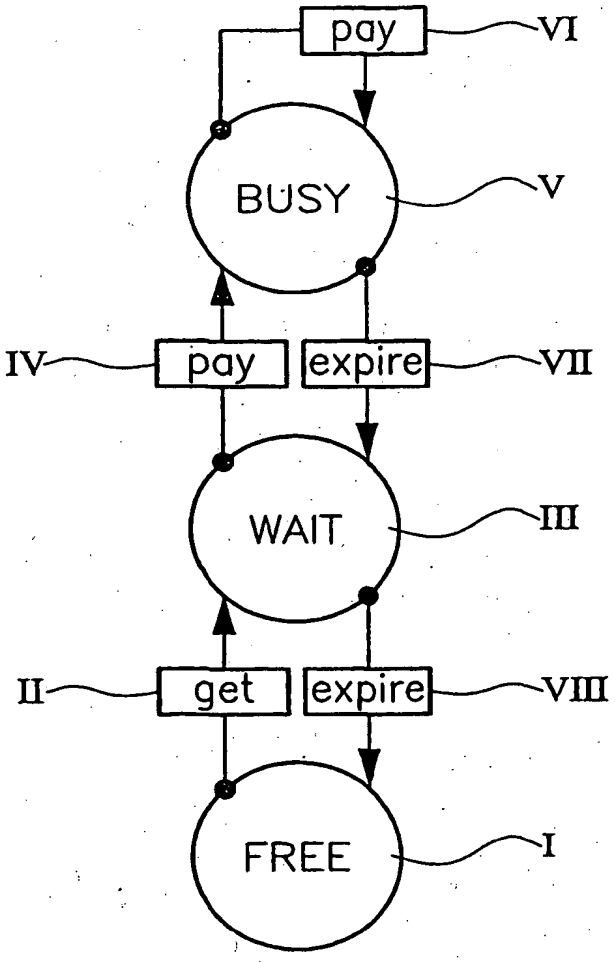

pay
VI
BUSY
V
IV
pay
expire
VII
WAIT
III
II
get
expire
VIII
FREE
I

FIG.2

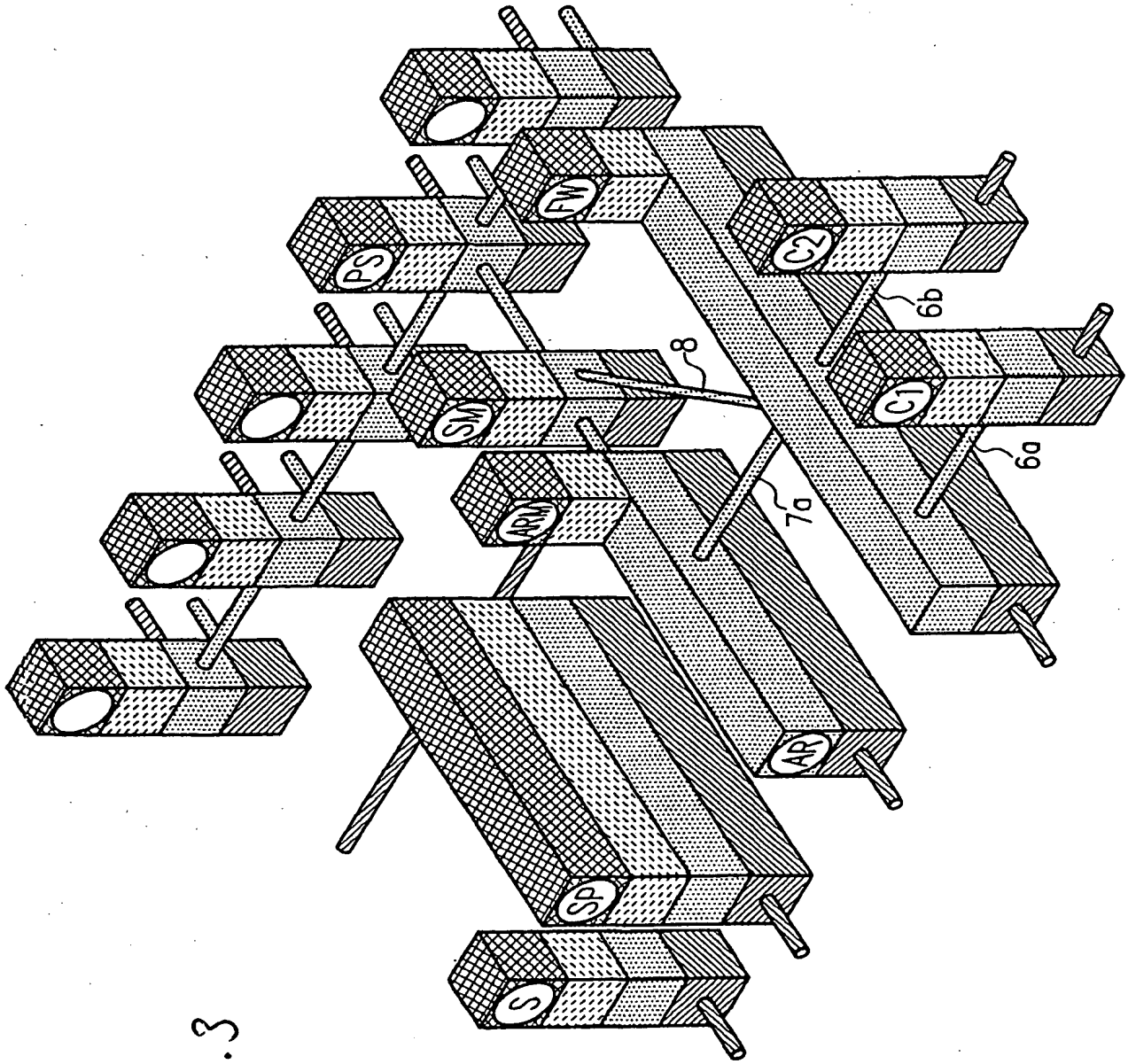


FIG.3

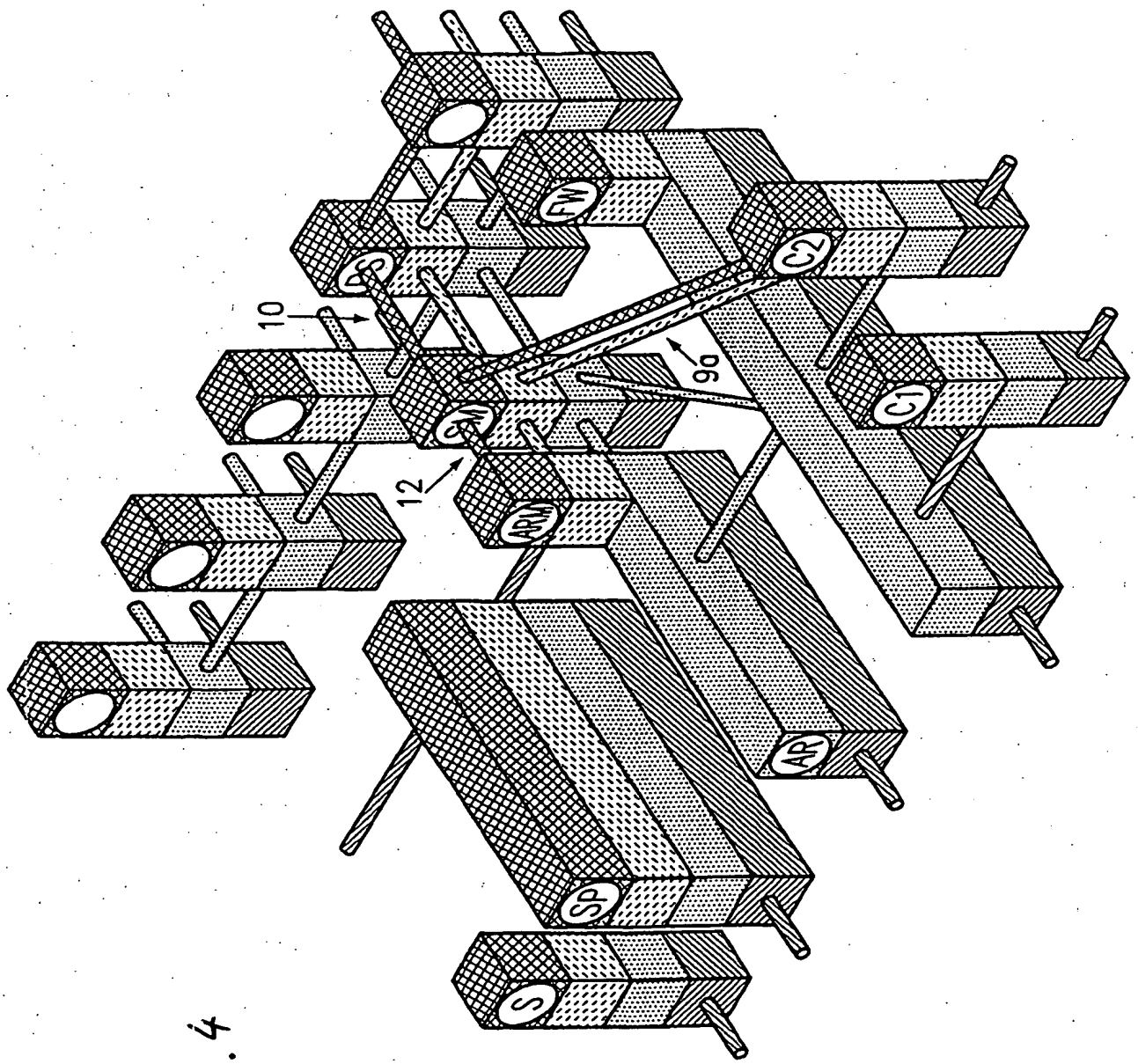


FIG. 4

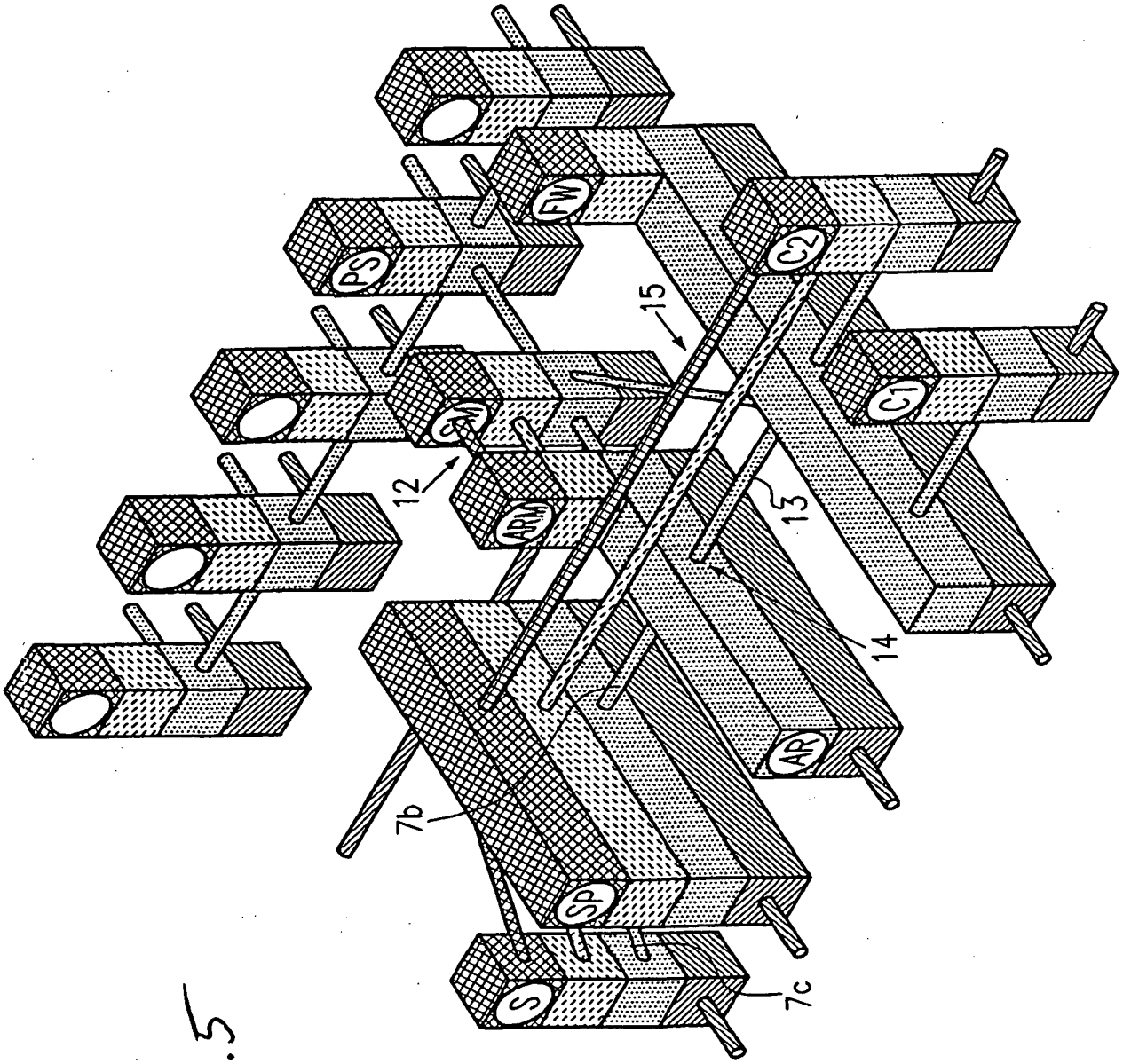


FIG.5

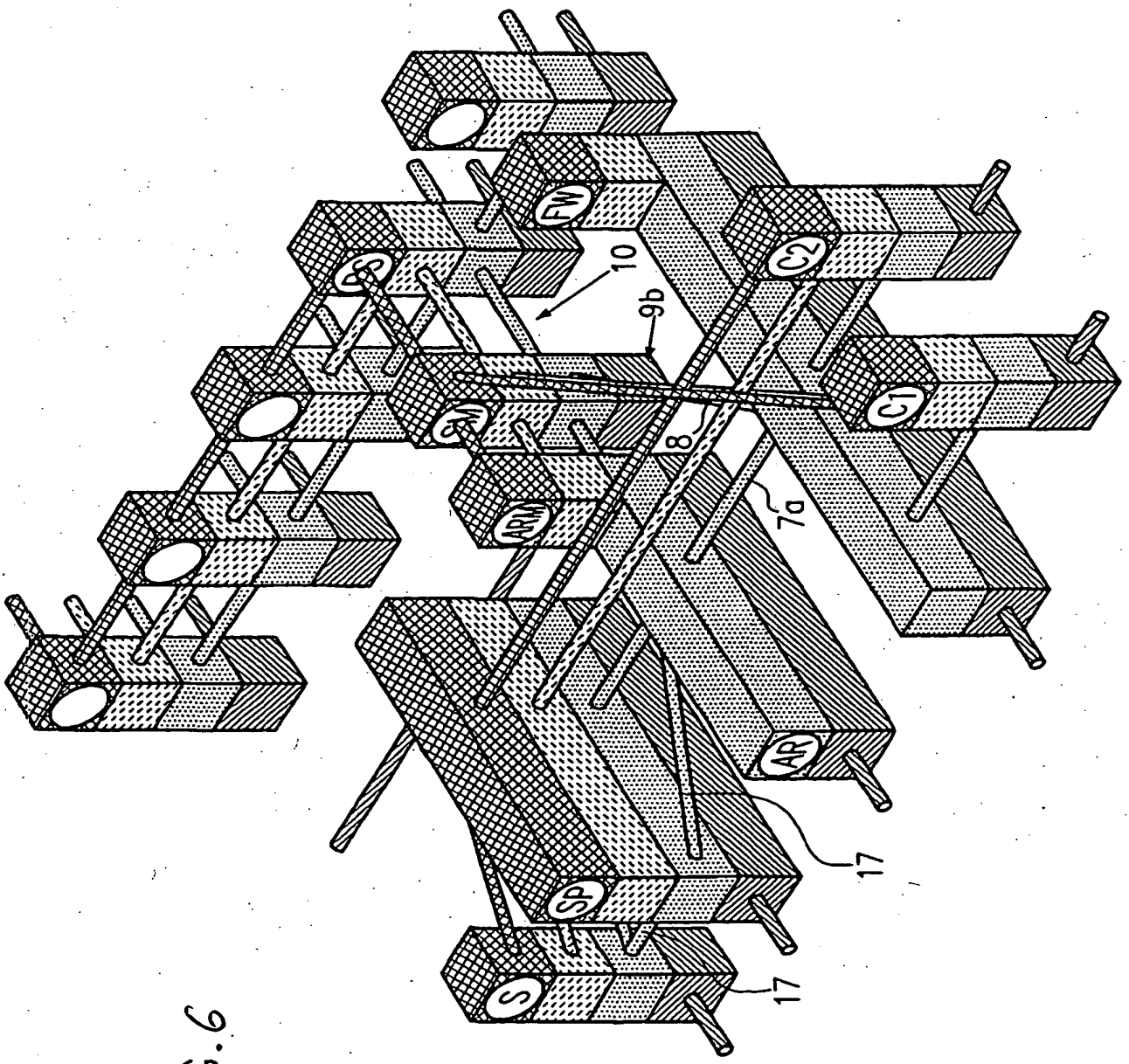


FIG. 6

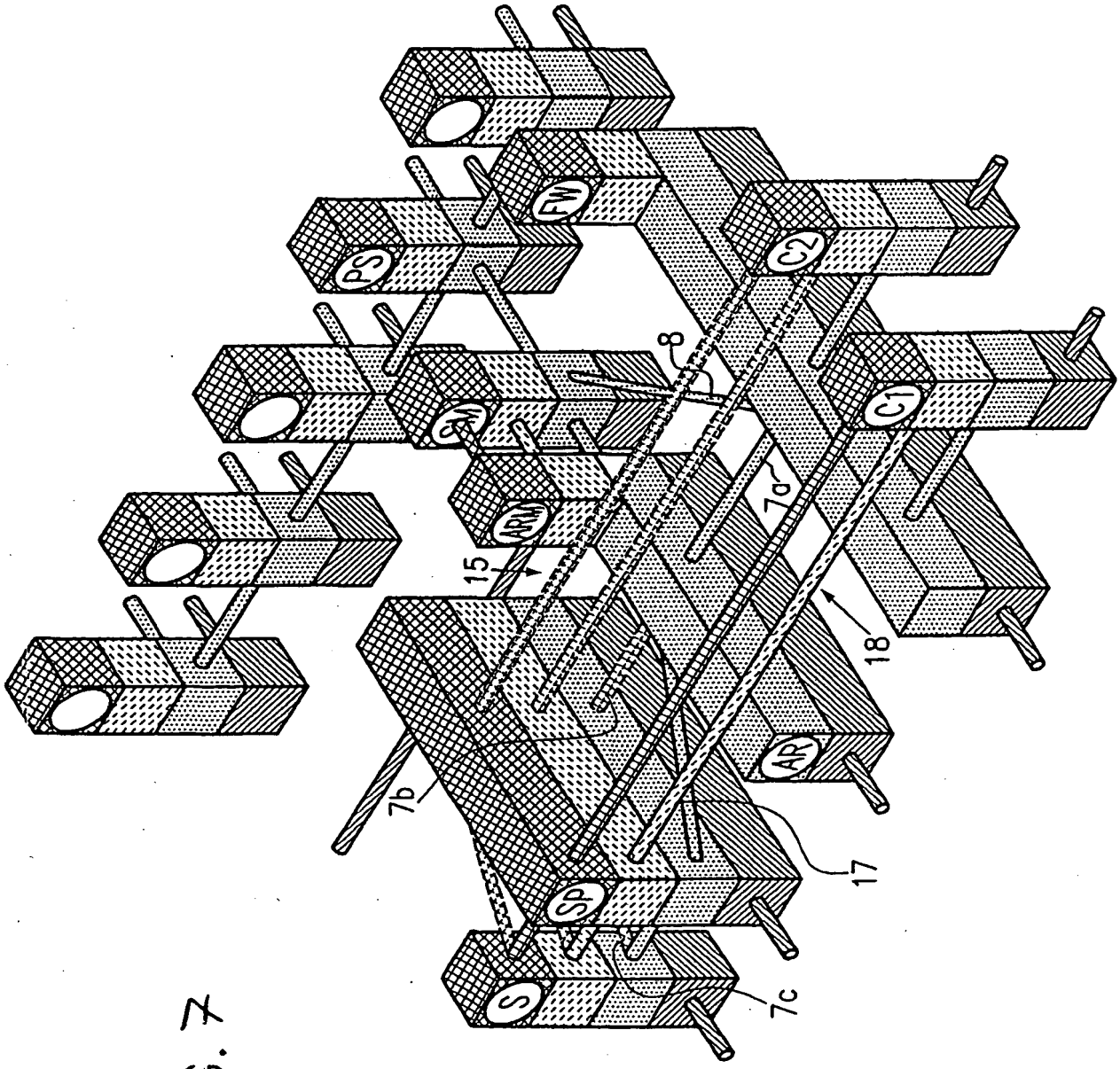


FIG. 7

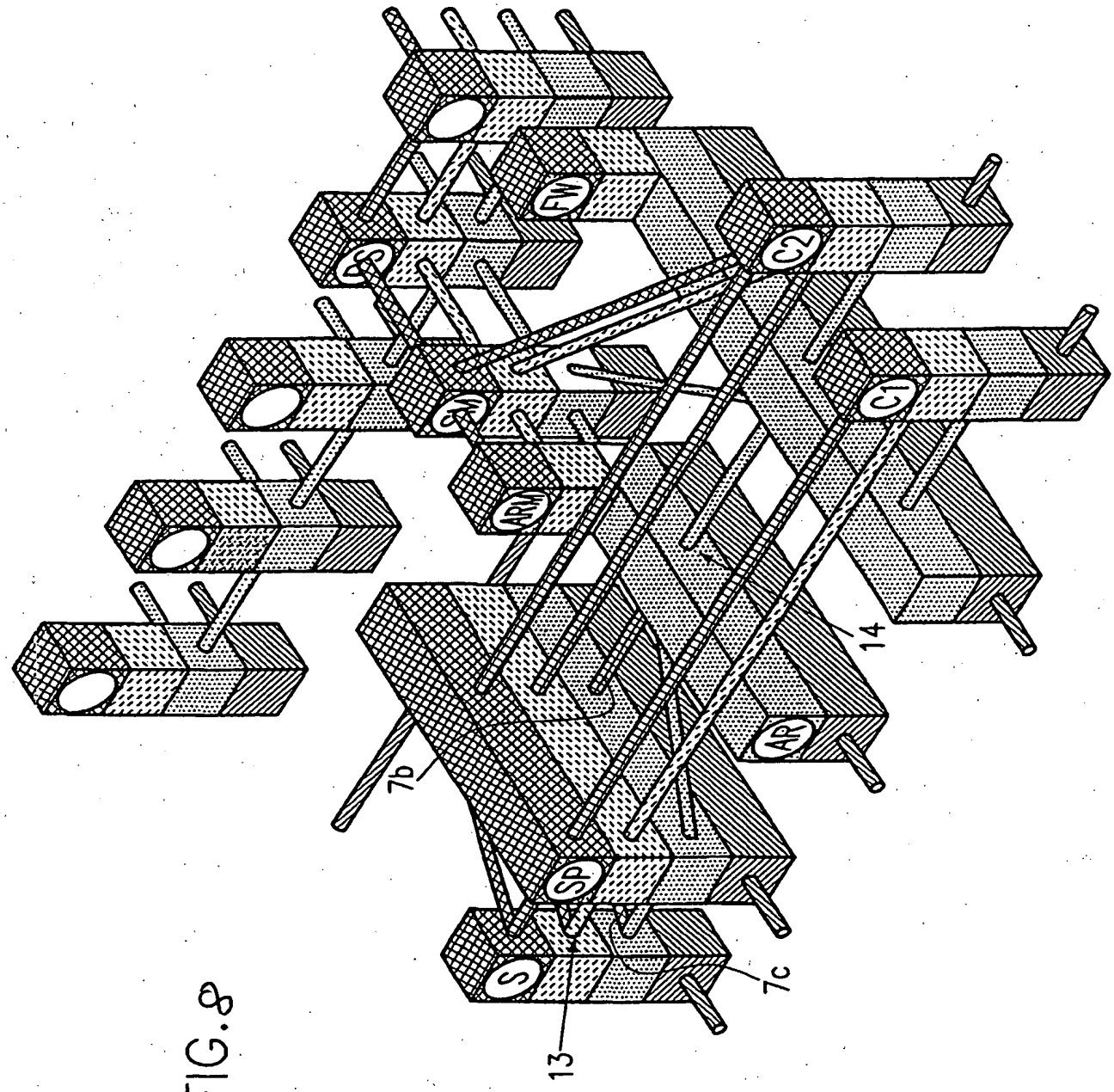


FIG.8

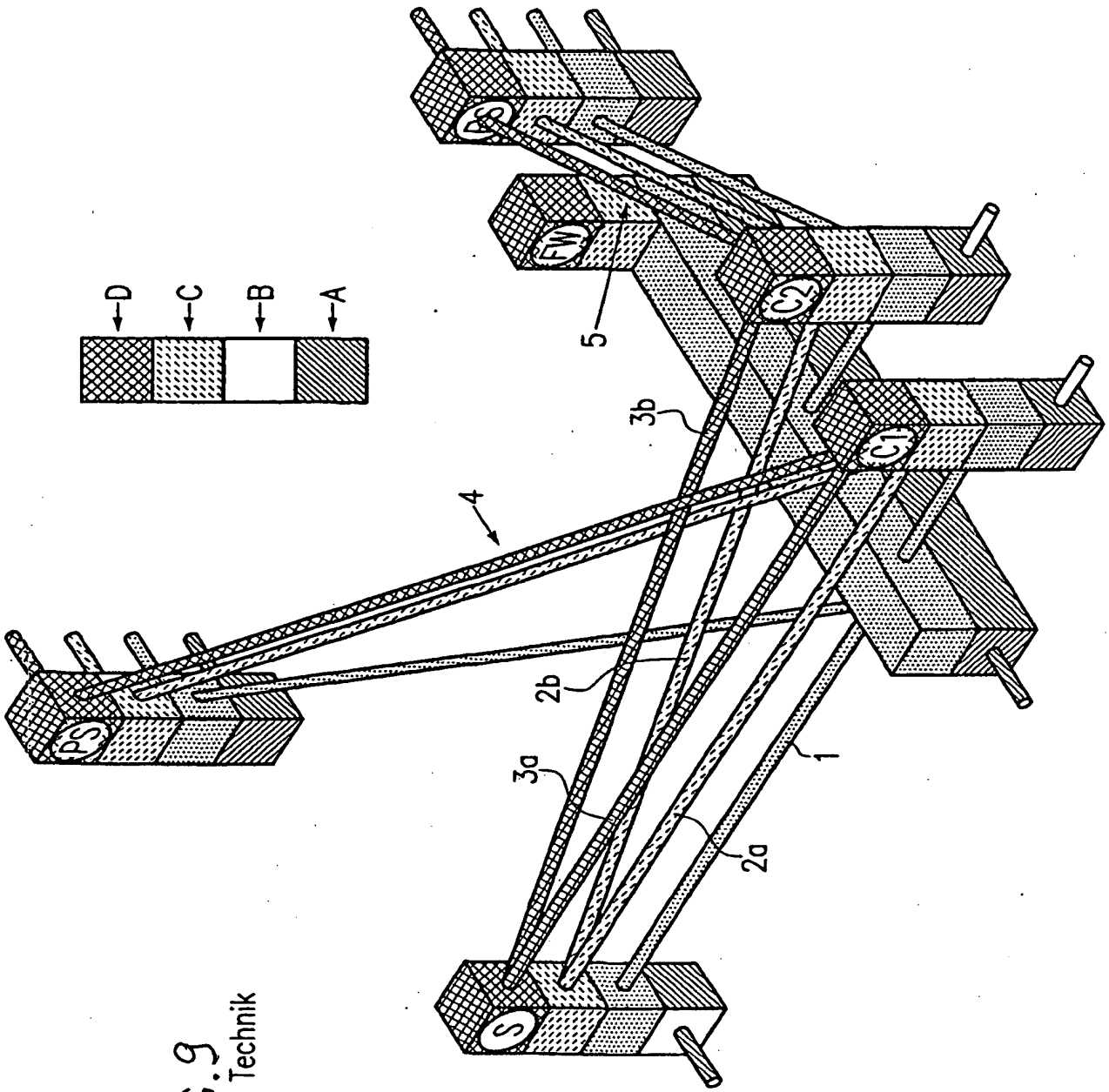


FIG.9
Stand der Technik

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- [x] BLACK BORDERS
- [ ] IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- [x] FADED TEXT OR DRAWING
- [x] BLURRED OR ILLEGIBLE TEXT OR DRAWING
- [ ] SKEWED/SLANTED IMAGES
- [ ] COLOR OR BLACK AND WHITE PHOTOGRAPHS
- [ ] GRAY SCALE DOCUMENTS
- [ ] LINES OR MARKS ON ORIGINAL DOCUMENT
- [x] REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- [ ] OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.